REMARKS

Claims 1, 3, 4, 6, 10 and 11 have been amended. No new matter is added. Accordingly, claims 1-13 are pending in the present application.

Reconsideration and allowance are respectfully requested in view of the following remarks.

Claim Rejection Under 35 U.S.C. § 101

Claims 1-10 are rejected under 35 U.S.C. §101 for allegedly being directed to non-statutory subject matter. Specifically, it is asserted in the Office Action that the claimed method can be performed via a computation using a piece of paper and pencil.

For clarification, claim 1 is amended to recite a cryptographic method during which an integer division of the type q = a div b and r = a mod b is performed in a processor of an electronic device, as suggested in the Office Action.

In view of the foregoing, it is respectfully requested that the rejection of claims 1-10 under 35 U.S.C. §101 be withdrawn.

Claim Rejection Under 35 U.S.C. § 112

Claims 3, 6, 10 and 11 are rejected under 35 U.S.C. §112, second paragraph, as allegedly being indefinite. Specifically, it is asserted in the Office Action that the meets and bounds of the claims cannot be readily ascertained. The Office Action specifically asserted that one of ordinary skill in the art cannot reasonably identify an appropriate input bound of "Input : $a = (0, a_{m-1}, \ldots, a_0)$" recited in the claims. Applicant respectfully disagrees.

The method steps in claims 3, 6, 10 and 11 are written in a format that is well understood by one of ordinary skill. For example, section 14.20 of the Menezes reference cited in the obviousness rejection below specifies input as "INPUT: positive integers $x = (x_t \ldots x_1x_0)_b$, $y = (y_t \ldots y_1y_0)_b$", which is a similar format used in the claims specifying the input.

Neverthless, for clarification, claims 3, 6, 10 and 11 are amended to describe the various operations and variables used in the steps of the claimed method.

In view of the foregoing, it is respectfully requested that the rejection of claims 3, 6, 10 and 11 under U.S.C. §112, second paragraph, be withdrawn.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-13 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Menezes ("Handbook of Applied Cryptography," hereinafter "Menezes") in view of Drexler et al. (U.S. Patent Application Publication No. 2003/0061498, hereinafter "Drexler"). Applicant respectfully traverses the rejection.

Exemplary embodiments of the present invention relate to an integer division method that is secured against covert channel type attacks. Covert channel attack includes an attack based on a physical quality measurable from outside the device and whose analysis makes it possible to discover data contained and manipulated in processing operations performed in a device. Physical quantities that are exploited during attacks include execution time, the current consumption, the electromagnetic field radiated by the part of component used for executing the calculation, etc. These attacks are based on the fact that, during the execution of a method, the manipulation of a bit leaves a particular imprint on the physical quantity in question,

according to the value of this bit and/or according to the instruction. For example, a method including iterations is sensitive to covert channel attacks if at each iteration of the method, the number of operations performed during the iteration varies according to the result bit obtained during the iteration.

According to exemplary embodiments of the present invention, the same operation is performed regardless the value of the bit obtained so that the method is secured against covert channel attacks. Claim 1 recites a cryptographic method during which an integer division of the type q = a div b and r = a mod b is performed in a processor of an electronic device, the method comprising, *inter alia*,

(i) performing a partial division of a word A, comprising n bits of the number a, by the number b to obtain a bit of the quotient q, wherein at least one of the numbers a and b comprises secret data; and

(ii) repeating step (i) for m-n+1 iterations with the same number and type of operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q.

Menezes does not disclose an integer division method with the same operations being performed at each iteration of obtaining a bit of the quotient, as described in claim 1. Referring to section 14.20 of Menezes, the disclosed Multiple-precision division method includes the following steps:

3. For i from n down to $(t+1)$ do the following:
   3.1 If $x_i = y_t$ then set $q_{i-t-1} \leftarrow b-1$; otherwise set $q_{i-t-1} \leftarrow \lfloor (x_i b + x_{i-1})/y_t \rfloor$.
   3.2 While $(q_{i-t-1}(y_t b + y_{t-1}) > x_i b^2 + x_{i-1} b + x_{i-2})$ do: $q_{i-t-1} \leftarrow q_{i-t-1} - 1$.
   3.3 $x \leftarrow x - q_{i-t-1} y b^{i-t-1}$.
   3.4 If $x < 0$ then set $x \leftarrow x + y b^{i-t-1}$ and $q_{i-t-1} \leftarrow q_{i-t-1} - 1$.

According to the method in Menezes, the operations performed at one iteration might be different from another iteration. For example, according to step 3.2, the number of operations performed during the iteration varies according to specific values of q_{i-t-1} during that iteration. Accordingly, Menezes does not teach or suggest a cryptographic method during which an integer division is performed, the method including repeating step (i) for m-n+1 iterations with the same number and type of operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q, as recited in claim 1.

Drexler, relied upon for allegedly disclosing that at least one of the numbers a and b comprises secret data, and generating encrypted and decrypted data in accordance with said quotient, does not remedy the above-noted deficiencies of Menezes.

In view of the foregoing, claim 1 is patentable. Claims 2-13 are patentable at least because of their dependency from claim 1.

CONCLUSION

From the foregoing, further and favorable action in the form of a Notice of Allowance is respectfully requested and such action is earnestly solicited.

In the event that there are any questions concerning this amendment, or the application in general, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: October 23, 2009

By: Weiwei Y. Stiltner
Weiwei Y. Stiltner
Registration No. 62979

Customer No. 21839

703 836 6620